Message

From: Edward Cunningham [redacted]@google.com]
Sent: 8/15/2018 3:13:57 PM
To: Purnima Kochikar [redacted]@google.com]; Bill Bilodeau [redacted]@google.com]
Subject: Fwd: Vulnerability report: Fortnite Installer downloads on Android are vulnerable to hijacking

Bill: can you send a brief note to your Epic contact (the Fortnite studio head I believe?) noting that our security team has reported a vulnerability and directing them to https://issuetracker.google.com/112630336 (Epic internal ticket **VLN-179**). No need to mention any specifics about the vulnerability itself.

Purnima: feel free to reach out to Mark Rein as you see fit. The internal ticket number VLN-179 may be handy for them.

Ed

---------- Forwarded message ----------
From: **Brendan Boyle** <[redacted]@epicgames.com>
Date: Wed, Aug 15, 2018 at 3:58 PM
Subject: Re: Vulnerability report: Fortnite Installer downloads on Android are vulnerable to hijacking
To: [redacted]@google.com
Cc: Security Bugs <[redacted]@epicgames.com>

Hey All,

I've sent this to our engineering team for further review and updated the Google Issue tracker ticket. Internal tracking ticket is VLN-179.

Thanks,
Brendan

On Wed, Aug 15, 2018 at 10:04 AM 'Edward Cunningham' via Security Bugs [redacted]@epicgames.com> wrote:

> Hi Epic Games security team,
>
> We've discovered a vulnerability in the Fortnite Installer on Android.
>
> I've filed a bug on the Google Issue Tracker here (copied below), which is currently restricted to members of [redacted]@epicgames.com. I can also directly add any individuals at Epic Games for whom this is relevant - just let me know.
>
> You're welcome to update that issue directly or use your own internal process. **Please note that the bug is subject to a 90-day disclosure deadline. After 90 days elapse or a patch has been made broadly available, the bug report will become visible to the public.**
>
> Thanks,
>
> Edward
> (Android Security team)
>
> **Report:** https://issuetracker.google.com/112630336

EXHIBIT 8576

The Fortnite APK (com.epicgames.fortnite) is downloaded by the Fortnite Installer (com.epicgames.portal) to external storage:

```
dream2lte:/ $ ls -al
/sdcard/Android/data/com.epicgames.portal/files/downloads/fn.4fe75bbc5a674f4f9b356b5c90567da5.Fortnite/
total 73360
drwxrwx--x 2 u0_a288 sdcard_rw     4096 2018-08-15 14:38 .
drwxrwx--x 3 u0_a288 sdcard_rw     4096 2018-08-15 14:38 ..
-rw-rw---- 1 u0_a288 sdcard_rw 75078149 2018-08-15 14:38 x1xlDRyBix-YbeDRrU2a8XPbT5ggIQ.apk
-rw-rw---- 1 u0_a288 sdcard_rw    31230 2018-08-15 14:38 x1xlDRyBix-YbeDRrU2a8XPbT5ggIQ.manifest
```

Any app with the WRITE_EXTERNAL_STORAGE permission can substitute the APK immediately after the download is completed and the fingerprint is verified. This is easily done using a FileObserver. The Fortnite Installer will proceed to install the substituted (fake) APK.

On Samsung devices, the Fortnite Installer performs the APK install silently via a private Galaxy Apps API. This API checks that the APK being installed has the package name com.epicgames.fortnite. Consequently the fake APK with a matching package name can be silently installed.

If the fake APK has a targetSdkVersion of 22 or lower, it will be granted all permissions it requests at install-time. This vulnerability allows an app on the device to hijack the Fortnite Installer to instead install a fake APK with any permissions that would normally require user disclosure.

A proof-of-concept screen recording can be found here.

Using a private internal storage directory rather than external storage would help avoid this vulnerability: https://developer.android.com/guide/topics/data/data-storage#filesInternal

See also this recent blog from Check Point: https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/